AD-A105 182 RAND CORP SANTA MONICA CA F/G 9/2
SECURITY, PRIVACY, AND NEW TECHNOLOGY,(U)
JAN 81 W H WARE
UNCLASSIFIED RAND/P-6606 NL

END
DATE FILMED
10-81
DTIC

(6) SECURITY, PRIVACY, AND NEW TECHNOLOGY

(10) Willis H. Ware

(12) 17

(11) January 1981

(14) RAND/P-6696

The Rand Paper Series

Papers are issued by The Rand Corporation as a service to its professional staff. Their purpose is to facilitate the exchange of ideas among those who share the author's research interests; Papers are not reports prepared in fulfillment of Rand's contracts or grants. Views expressed in a Paper are the author's own, and are not necessarily shared by Rand or its research sponsors.

The Rand Corporation
Santa Monica, California 90406

SECURITY, PRIVACY, AND NEW TECHNOLOGY*

INTRODUCTION

Ladies and gentlemen, it is a genuine pleasure for me to be here this morning. As the chairman has suggested, I have on many occasions talked to groups in the United States, but unfortunately my interaction with the European community is not extensive. Thus, I am particularly appreciative of Honeywell-Bull for inviting me to this symposium.

I want to offer several ideas for your consideration, including possible effects technology may have on privacy and security in the future. I will not address either economic or political aspects, and I hope my comments will integrate some of the things that you have already heard.

Everyone of us fully understands that our respective countries have made a commitment to computer technology; and it has become so central to our way of life and our life's affluence that there is no turning back. We could not do without computers except by seriously degrading our quality of life, our personal opportunities, our recreational and travel conveniences, and the whole fabric of the modern world. In fact, the world has become so complex that there is no longer a way to run it without computer technology; it could no longer be operated with paper and pencil and the green eye shades of the accountant. At the same time, each of us perceives the pace of technology all around in communications, microprocessors, and solid-state electronics. We see new applications; we see enlargements of old applications. There are electronic fund systems at the consumer level,

---

*Presented at First International Cii Honeywell-Bull Symposium on Computer Security and Privacy--Top Secret 81 at Monte Carlo, Monaco, January 28, 1981.

electronic mail for the individual, and computers in retail shops. Software is also available at the retail store and point-of-sale systems are becoming prevalent in stores and shops. The consequence of such developments is that more and more of one's lifestyle and life activities will be documented in some recordkeeping system.

As computers have become central to the corporation, to the government agency, and also to the country, it is not surprising that they have become attractive opportunities for wrongdoing. Anything which has great enough value will ultimately become a focus for misdeeds. We hear about stealing computer time, stealing goods and money, and disrupting a company. Ultimately a country might be brought to its knees. Sometimes such events involve manipulating software; sometimes an undesirable event is simply discovering an anomaly in the system and exploiting it for personal gain. Sometimes it is physical destruction of the hardware, or the data files, or the software.

From the privacy point of view, proliferation of technology is leading to evermore accumulation of information about people. It can be used in new but perhaps wrongful ways; there are bound to be new privacy issues. If it is so, then security also will have new issues as well because the two are related. How ominous is the future? Is there really a growing threat? If so, what is it? What is the role of technology in it?

As I have listened to the symposium the last two days, it is clear that it is interested strongly in computer security and computer crime. I will therefore emphasize these items more than I had originally intended.

TERMINOLOGY

Let us first be precise about terminology because it may differ in Europe compared to the United States. Security or computer security includes all the things that must be done to protect a computer system, together with its people, data, equipment and communications, against a defined threat, plus access controls to make sure that the system provides information only to people authorized to receive it. In contrast, privacy relates to the use of information about people, especially how it is used to affect an individual. Privacy, as the term is currently used, addresses the relationship between an individual and some recordkeeping system, and implies that personal information must be protected and used appropriately. Thus, one must do a thorough job on security and be able to protect information properly before he can feel ready to respond to a privacy mandate.

Security is a technical matter together with policy, procedural, and administrative aspects. Privacy is an information use matter as required by law or stipulated by corporate conscience. As generally understood, computer security safeguards include technically

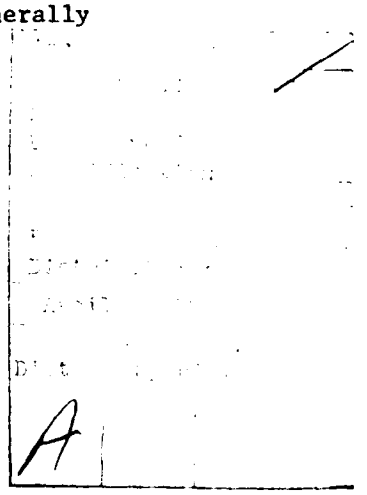
- o those in hardware
- o those in software
- o those in communication

plus

- o procedural controls
- o personnel controls
- o management controls

all

- o embedded in an administrative framework that monitors all such controls and makes certain all continue to operate properly.



Finally, confidential describes information that is sensitive for some reason and therefore requires protection and controlled use. Thus, confidential information is protected by computer security safeguards. If the information is about people, its use may be controlled by privacy legislation. A computer system that has proper controls and safeguards is sometimes called a trusted computer system.

COMPUTER CRIME

Let us first address computer crime, which was a subject of intense discussion yesterday. It should not be a surprise that computer crime exists. As a matter of fact, as far as I can see, the only surprise is that we are surprised. The computer is a valuable object; software is a valuable object; computers do important things; they will automatically become targets for abuse. Why has it materialized so much in recent years? Why haven't we done better in foreseeing and combating computer crime?

I would suggest that part of it is that law enforcement officials have been slow in getting the special training that is needed. Prosecutors have been unwilling to tangle with a very complex topic both unfamiliar and highly technical, and for which there is little guiding prior case law. The victims of computer crime are embarrassed to reveal what has happened, or they worry about public image. Passage of time also plays a role. As systems operate over longer periods of time, potential troublemakers learn more about them and get new ideas of how to abuse them.

Let me say clearly that I do not argue against new legislation, but let me say equally strongly that I do caution that we be very

careful about what features we design into new law. Fraud is fraud, whether it is committed by computer, by paper and pencil, or by word of mouth. On the other hand, it is one thing to steal an empty roll of magnetic tape as opposed to stealing a role of magnetic tape full of valuable programs. Each is a theft of an object, but the second contains intellectual property, a genuinely new dimension of thievery that has been made prominent by the computer. Our laws must address such subtleties.

There are other novel and unique aspects of criminal acts that arise as a result of a computer; these, too, must be accommodated in law. New law need not concern itself with things already adequately covered in existing statutes even though the situation may be magnified through the use of the computer. Let us be cautious as we move forward; let us not panic into a lot of new legislation that we may later see as useless or even troublesome.

COMPUTER SECURITY

Now computer security. Ten years ago I was rather optimistic and felt that the matter would move ahead rapidly. Why have we not progressed more rapidly? Why have we not the safeguards to protect against crime and against similar problems? There are many reasons. First, most of the operational systems of today are either first generation ones, or are evolutions of first generation ones. They were never designed with security safeguards in the first place simply because system designers were not thinking about the matter fifteen years ago. Whatever safeguards exist in the systems of today have been retrofitted to an existing design. Having been put in after the

fact, they cannot be as comprehensive as integral ones that are installed as part of the initial design.

Secondly, manufacturers have been slow to provide hardware and software with appropriate safeguards in each. However, let us not blame it all on them because they respond to the marketplace. You, the customers, have been slow in signaling to the manufacturers that security safeguards are important, are needed, and will be paid for. Furthermore, technologists have generally not been aggressive in pushing the art already in hand.

Very importantly, management has been a major impediment. Managers who buy insurance, who remember to lock the door at night, and who understand the need for an external audit of their fiscal accounting process simply seem baffled by the computer. Managers do not seem to appreciate that the computer is the vault for their valuable information, just as the bank vault is a safe place for currency.

COMPUTER DEFENSE

I would suggest that we would be better off and be more persuasive to management, if we regarded computer crime as a form of warfare, and if we talked about computer defense rather than about computer security. If the problem were phrased that way, management might be more responsive. How do we get ahead with the problem?

It starts with a commitment from the corporation or from the government agency to do the job, but the commitment must include money. Some things that will have to be done will require funds, especially if a particular installation is largely unprotected. Such costs can be thought of as a form of insurance that defends and protects a computer

system against undesirable negative events. On the other hand, a corporation or a federal agency cannot spend unlimited funds. It becomes necessary to assess the threats against the computer system to be protected, and then to use technology as appropriate to guard against them.

Management must understand that computer defense is not a static matter, but a dynamically changing one. The threat against a computer system can change dramatically in a very short time, and appropriate defenses may have to be implemented correspondingly quickly. Funds will be required continuously, just as insurance premiums have to be paid every year. Management must understand such a point of view; it must understand that protecting a computer system is analogous to the deterrence of law enforcement against criminals or of military defense forces against an opponent's attack.

THE SCENARIO

In regard to threat assessment, I would like to comment about the role of scenarios. It is not new to suggest that a scenario is an appropriate mechanism for assessing threat. It is a technique that the contingency planner has always used. The scenario is valuable because it suggests what might happen, rather than predicting what will happen. Therefore, it alerts us to possibilities against which we can erect proper defenses so that the situation envisioned in the scenario is averted. The military planner has always used scenarios to devise defense forces, but he has a unique advantage. He can see the country against which he must defend; he can observe its forces in training; he can consider the thrust of its technology; he can see

how geography and terrain constrain an opponent's options. All such inputs can go into his plans.

In contrast, the computer defense planner does not have such opportunities. He cannot see the individual planning to create some software aberration, nor can he observe the clerk who notices some system anomaly. For him, it is more like the criminal's inside job; he cannot anticipate its details. Therefore, he has to imagine what might happen for which a scenario is valuable. He has to study other instances of attacks against computer systems. He has to exchange information with professional colleagues and take every advantage of the technology that is available.

Moreover, he has to do it all at a cost that his superiors will accept; we have already noted that cost is a stumbling block. Furthermore, the computer defense planner has less than a decade of experience regarding what can happen; the military planner has several centuries of experience with warfare.

DATA EXPOSURE

Now turn to the future. As we enlarge systems that we already have or as we use them in different ways, there will be new consequences. There will be other consequences of new systems that we have yet to design. Address the first issue and think for a minute about what I will call data exposure; I will illustrate it with an example. In 1975, the tax authorities in America proposed to create a nationwide network for handling tax information. It was to have several thousand terminals and many processing centers, all networked together. The effect would have been to significantly increase the exposure of tax

information. There would have been more tax information in transit on communication lines; there would have been more access to tax information by agents at terminals. Fortunately, the United States was not ready for such a move in 1975 and it did not happen.

However, as industry and technologists move ahead with both old and new systems, I would suggest my first alert:

> Networking will significantly increase data exposure and thus increase the risk of a breach of confidentiality or privacy invasion.

Computer defenses will be needed at the network level, a much harder job than defenses for a centralized self-contained system.

A NEW PRIVACY ASPECT

Continuing with the tax example, let me suggest a new dimension of privacy that is upon us. The classical privacy issue, as it is talked about in this symposium and elsewhere, concerns itself with the relationship between an individual and a recordkeeping system. Usually the recordholder can do new things with the data if the individuals in question consent. In 1976, a new law in the United States established that all tax information would be confidential and would have to be protected properly. Moreover, that same law defined very precisely what uses might be made of tax information. Some of the old uses were denied under the new law; for example, law enforcement authorities need a court order to obtain it.

Here is a new dimension of privacy. The individual may still see his tax record under privacy law, but in addition all uses of the total data base of tax information are now very carefully governed by a

different law. In effect, the 1976 tax law has defined what the Congress of the United States, and therefore the people of the United States, consider to be societally accepted uses of tax information. It is a new dimension of privacy in that the use of a whole body of information is constrained by law, rather than the individual participating in determining the uses of his record. I would suggest as a second alert that:

> We must be sensitive, as we move ahead, to the possibility that we may, especially with new systems, create bodies of data about people that will need specific new legal protection.

GATEKEEPING

Let me suggest another latent issue. There is a so-called gatekeeping aspect of computer systems. It concerns the idea that an individual may or may not have access to certain privileges depending on some record that is kept about him in a computer. The common example is the credit record; it influences strongly whether an individual can "walk through the gate" to a new automobile, a new house, or even to an education. Already operating in the United States are computer-based schemes that automatically make decisions about credit worthiness of an individual, using only publicly available and societally accepted information for the purpose. The individual is never asked a question, but one day he receives in the mail an offer of credit or of a credit card. Such a scheme can discriminate against some classes of people in a very subtle way, and it will be hard to detect and hard to guard against. I would suggest as a third alert that:

> We must be very sensitive, as we move ahead, to the possibility that new systems, or old ones used in new ways, will inadvertently cause social discrimination.

It will be a difficult thing to detect because details of such inadvertent or deliberate actions will be deeply concealed in computer programs.

DATA PUDDLES

Think now about new things and consider electronic mail. The United States Postal Service is actively pursuing such a possibility; France is also. For such a system to work, not only must it transmit the contents of a message, but also it clearly must relate the sender of the message to the addressee. The system will have to retain such sender-addressee information for some period of time because messages are going to get lost, or messages will be missent, or there may be a law enforcement aspect, or there may be legislative oversight requirements, or there may arise a question as to actual delivery of a message. Inevitably the system will accumulate information about people which I have come to call "puddles of data." Such puddles do not exist for recordkeeping purposes, as we customarily use the term, but rather they exist just to make the system do what it is supposed to do. After the system has fulfilled its intended function, then the puddles will dry up and go away.

Consider what an attractive target for misdeeds such data puddles will become. They will clearly be of intense interest to law enforcement authorities. They may be of interest to lawyers looking for evidence. They will surely be of interest to government. Nonetheless,

data puddles will not be covered by privacy law because they do not contain a record used to make a decision about an individual. The United States Postal Service seems wholly insensitive to this matter; it seems unaware of the privacy and security consequences of what it proposes to do. Even worse, it proposes to transmit electronic mail information via satellite circuits on which anyone that chooses to can readily eavesdrop. In my view, the United States postal authorities should be pressing for new legislation that would give specific legal protection to all aspects of the electronic information associated with electronic mail service.

My fourth alert would suggest that:

> As government agencies and private organizations exploit all the new technology that we have, they may be insensitive or even indifferent to the privacy and security consequences of what they are doing.

The "data puddles" of an electronic mail system are an example of the new privacy dimension that I previously have suggested to you. Unless it were protected both technically and legally, the time honored secrecy of first class mail would be at risk. A similar situation is the point-of-sale system. It too will accumulate puddles of data about people and can easily become a source of privacy invasion or wrongful use of information about people.

My fifth alert is related.

> We must be very watchful for circumstances in which information about people has a marked increase in exposure or accessibility, and in such circumstances aggressively seek necessary legislation to protect such information.

TECHNOLOGICAL DEFENSES

Turn now to technology and some opportunities that it will afford for future computer defenses. A recent report from the Swedish Defense Ministry, the so-called SARK report, has suggested a number of national vulnerabilities that concern Sweden; I assume they will also be of concern to each other country. There is technology now here or soon coming that can help guard against such vulnerabilities.

One item of concern is the communication circuit that passes through another country and is controlled by it. I would suggest that satellite communications can handle the threat very adroitly, not the kind that we have today which require large ground stations, but rather the kind that is to be offered shortly by the Satellite Business Systems company in America. Its satellite circuits will go rooftop to rooftop without large ground stations so one can have point-to-point direct channels. Furthermore, SBS will offer to encrypt its transmissions so they will not be readable enroute.

Another SARK item of concern is the sensitivity of data bases that might fall into the hands of a future enemy, an issue of particular concern in Europe. I would suggest that encryption is a possible answer. It is dramatically simpler to destroy the key needed to decrypt an encrypted data base than to physically destroy all the magnetic tapes or all the magnetic discs on which the data base itself resides. As a matter of fact, I would suggest that the point just made is a powerful argument for computerizing sensitive information; the computer automatically and efficiently can carry out the necessary protective processes. In contrast, encrypting or decrypting of manual

records is slow and tedious, and the bulk of manual records makes it difficult and slow to destroy them.

A technology that might counter the vulnerability of individual computing centers is that of networking and distributed processing. Such techniques would obviously make it harder for a single attack to disable a company or a government; ultimately, the smaller and smaller computers that are coming will be advantageous because they can be easily hidden, more readily protected, and moved if necessary.

A NETWORK DEFENSE

Another technical idea is one that first came to me in regard to the National Crime Information Center that the FBI operates in America. The FBI wanted all fifty states to put criminal histories into the NCIC but most states refused, partly on legal grounds but partly because the states simply did not want the Washington government to have so much information. I would suggest that there is a technical way to mediate such a problem. One networks all fifty states together and includes Washington as a fifty-first state. Each state would be assigned the role of watchdog for all transactions among certain other states. One could, if wished, have each transaction between two states monitored by three, four, six other states. Perhaps all fifty would be assigned the role of watching all transactions with the FBI. We would have a distributed watchdog, so to speak.

In an arrangement such as this, it would take massive collusion for any member of the network to act improperly and attempt to accumulate a data base to which it is not entitled--exactly the concern that the NCIC faces with computerized criminal histories. In a way, the

idea really takes an essential aspect of democratic government and embodies it in a computer network, that of checks-and-balances. The idea is also an example of a computer system safeguard that is possible only in a network.

There are already tightly knit communities of interest that transcend national borders. Banking is one; law enforcement is another. One could network such a community of interest so that collectively it watched for offensive actions against all members of the network. So to speak, there would be a community awareness of the hostile actions rather than every member of the network having to watch for himself. Thus, the idea is an appropriate one to counter the extreme threat of one country electronically warring against the fund transfer system of another. Technology to make such an arrangement is here; we do not need any new inventions. Clearly though, it would take a very persuasive argument to move the banking community, for example, in such a preferred direction.

THE 1980s

In the 1980s, there is likely to be much ongoing public discussion of the cost of computer defenses and of the threats against computer systems. Such debates are likely to be very vocal for such systems as electronic mail or consumer-level fund transfer systems. In a way, it is unfortunate that the discussion will take place because it will mean that organizations are still unsure whether computer defenses and privacy matters ought to be accommodated in new system designs. It will mean that the general problem is not yet resolved; it will mean that government and corporations do not yet understand that privacy

and security safeguards are mandatory, must be automatically included in systems from the start, and not thought of as an optional choice.

It would be further regrettable because the evidence to date suggests that it is not all that expensive to do a good computer defense job. There are obvious one-time costs such as building appropriate rooms with adequate locks and doors, providing fire protection, and there are ongoing operational costs. In the large, it is not excessively expensive and therefore we should not argue about it; we should simply attend to computer defenses and privacy.

All of us here have a unique awareness of privacy, security, and confidentiality issues; we understand it better than most. We have a special obligation to be very vocal about such matters; we have a special obligation to be very persuasive in our industrial environments. We have a special obligation to be influential with our governments; and we have a special obligation to protect the future in the direction that we are talking about in the symposium. If I were to guess today, I would say that in 1990 we will probably all be here again, and talking about many of the same subjects. There will be new twists to old subjects; there will be slightly different nuances; and the systems of concern will be different. It has already been ten years since responsible people first identified the problem. I can sometimes feel pessimistic because we have not properly dealt with it. The effect that I did not adequately appreciate in the past was the inertia of government and industry, and their unwillingness to face the reality of what can happen.

I hope that my thoughts today have been useful to you. I trust that the alerts, as I have called them, have increased your awareness of things that might otherwise not have been noticed. I have appreciated the opportunity to speak with you this day and to have shared our time together.


ATE
LME